KEY SCHEDULE ALGORITHM BASED ON COORDINATE GEOMETRY OF A THREE-DIMENSIONAL HYBRID CUBE

MUHAMMAD FAHEEM MUSHTAQ

A thesis submitted in partial
fulfillment of the requirement for the award of the
Degree of Doctor of Philosophy

Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia

JANUARY 2019

I dedicated this research work to my mother, father, wife, brother and sisters whose sincere prayers and efforts make it possible for me to fulfill their utmost desire.

ACKNOWLEDGEMENT

In the name of Allah, the most beneficent and the most merciful. All praise to the Almighty Allah, for the good health and wellbeing that were necessary to complete this research work. At this moment, first of all, I would like to express my special gratitude to my soft-hearted, kind and loving supervisor Associate Prof. Dr. Sapiee Jamel who treated us in the best way possible and prepared us for the real-world challenges. I never forget his sincere guidance, motivation, immense knowledge and ideas throughout my research work. His constructive comments and suggestion during my Ph.D. study contributed to make this research work successful. In fact, during the whole project whenever the clouds of sorrow, despair and anxiety darkened my life, he behaved like a true mentor to shun all hurdles. I would like to thank him for all the trips around Malaysia that he organized for us and provide fishing trainings, thanks for unforgettable memories. I am really thankful to him for giving me the opportunity to be awarded Postgraduate Research Grant from ORICC, UTHM that provides financial assistance to conduct my research.

I am also grateful and my sincere appreciation to the FSKTM's Dean, Prof. Dr. Nazri Mohd Nawi and other faculty/staff members for providing a research-oriented environment and educational facilities. I would like to thank to all FSKTM postgraduate fellows for the moral supports, knowledge sharing, and company given to me throughout my PhD journey. I would like to express my special gratitude to Centre for Graduate Studies (CGS), UTHM who provide me the opportunity to serve as the Vice President of Graduate Student Association (GSA). I got a wonderful experience to work with CGS and UTHM during my journey in GSA. I am heartily thankful to one and all, who directly or indirectly, have lent their helping hand in this study, may the Almighty Allah reward you all.

Finally, the sincere gratitude to my dearest family members especially my beloved wife Ms. Urooj Akram for her endless support, emotional help, prayers, encouragement, care and kindness during my study. All of you are the main reason that always motivated me to do the best.

ABSTRACT

Cryptographic algorithms play an important role in information security where it ensures the security of data across the network or storage. A key schedule algorithm is the mechanism that generates and schedules all session-keys for the encryption process. The 2-dimensional hybrid cube is generated based on permutation and combination of integer numbers that are utilized in the construction of encryption and decryption key in the non-binary block cipher. The generation of key space by using the 2-dimensional hybrid cubes are not sufficient to resist attacks and could easily be exploited. Therefore, the large key space is more desirable to resist any attack on the secret key. This research proposed a new Key Schedule Algorithm based on the coordinate geometry of a Hybrid Cube (KSAHC) for the non-binary block cipher. By using the three-dimensional hybrid cube in KSAHC transformation, encryption keys are represented as $n \times n \times n$ matrix of integer numbers and used in the development of the permutation and substitution of order 4 square matrix. Triangular Coordinate Extraction (TCE) technique has also been introduced to extract the coordinates during the rotation of Hybrid Cube surface (*HCs*) and plays an important role in the development of KSAHC algorithm. The Hybrid Cube Encryption Algorithm (HiSea) has been implemented to validate the encryption keys that are generated from the proposed algorithm. The strength of the keys and ciphertext are compared with the Advanced Encryption Standard (AES), HiSea, and Dynamic Key Schedule Algorithm (DKSA). The proposed KSAHC algorithm has been validated using the randomness test proposed and recommended by NIST, the average result of avalanche test is 93%, entropy is 0.9968, correlation assessment test is -0.000601 and having large key space 2.70×10^{67} keys that makes the Brute Force attack difficult and time-consuming. Therefore, it can be concluded that the strength and validity of KSAHC algorithm have been enhanced as compared to other algorithms and can serve as the alternative algorithm in designing security systems.

ABSTRAK

Algoritma kriptografi memainkan peranan yang penting dalam keselamatan maklumat di mana ianya menjamin keselamatan data dalam sesebuah rangkaian atau storan. Algoritma jadual kekunci meupakan sebuah mekanisma yang menjana dan menjadual semua kekunci sesi bagi proses enkripsi. Kubus hibrid 2-dimensi dijana berdasarkan permutasi dan kombinasi nombor integer yang digunakan ketika pembentukan kekunci enkripsi dan dekripsi dalam blok cipher bukan binari. Penjanaan key space menggunakan kubus hibrid 2-dimensi adalah tidak memadai bagi menahan serangan dan dapat dieksploitasi dengan mudah. Maka, key space yang besar adalah lebih diperlukan bagi menahan serangan terhadap kekunci rahsia. Penyelidikan ini telah mencadangkan sebuah Algoritma Jadual Kekunci yang baharu berdasarkan koordinat geometri sebuah Kubus Hibrid (KSAHC) bagi blok cipher bukan binari. Dengan menggunakan kubus hibrid tiga dimensi dalam transformasi KSAHC, kekunci enkripsi diwakili sebagai matriks $n \times n \times n$ dengan nombor integer dan digunakan dalam pembentukan permutasi dan kombinasi bagi matriks empat segi susuanan 4. Teknik pengekstrakan koordinat tiga segi (TCE) juga telah diperkenalkan bagi mengekstrak koordinat semasa putaran satah-satah Kubus Hibrid (HCs) dan ianya memainkan peranan yang penting dalam penghasilan algoritma KSAHC. Algoritma Enkripsi Kubus Hibrid (HiSea) telah digunakan bagi mengesahkan kekunci enkripsi yang dijana menggunakan algoritma yang dicadangkan. Kekuatan kekunci dan teks cipher yang dihasilkan dibanding tara dengan algoritma Piawaian Enkripsi Lanjutan (AES), HiSea, dan Algoritma Jadual Kekunci Dinamik (DKSA). Algoritma KSAHC yang dicadang telah disahkan menggunakan ujian kerawakan yang dicadangkan oleh NIST, hasil pengujian longsor secara purata adalah 93%, entropi sebanyak 0.9968, pengujian taksiran korelasi ialah 0.000601 dan pemunyaan key space yang besar sebanyak 2.70×10^{67} kekunci yang menjadikan serangan Daya Kasar rumit dan memakan masa. Justeru, dapat disimpulkan bahawa kekuatan dan kesahan algoritma KSAHC telah ditambah baik berbanding lain-lain algoritma dan dapat diguna pakai sebagai algoritma alternatif bagi mereka bentuk sistem keselamatan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF PSEUDO-CODES

LIST OF SYMBOLS AND ABBREVIATIONS

HiSea	-	Hybrid Cube Encryption Algorithm
AES	-	Advance Encryption Standard
DES	-	Data Encryption Standard
MC	-	Magic Cube
KSAHC	-	Key Schedule Algorithm based on coordinate geometry Hybrid Cube
NIST	-	National Institute for Standard Technology
TOY100	-	TOY100 Encryption Algorithm
$\rightarrow$	-	Direct mapping
$\wedge$	-	And
$\in$	-	Element of set
$\forall$	-	For all element of set
Correlation (M, C)	-	Correlation between Message (M) and Cipher (C)
H (X)	-	Entropy of X
mod	-	Modulo
O	-	Center
L	-	Line
2D	-	Two Dimensional
3D	-	Three Dimensional
Q1 to Q4	-	Quarter 1 to Quarter 4
HCs	-	Hybrid Cube surface
IniFCol	-	Initialization face of column rotation
IniFRow	-	Initialization face of row rotation
CR_j	-	Column and Rows selection

LIST OF PUBLICATIONS

Journals:

(i) Muhammad Faheem Mushtaq, Sapiee Jamel and Mustafa Mat Deris (2017), "Triangular Coordinate Extraction (TCE) for Hybrid Cubes" Journal of Engineering and Applied Sciences. Vol. 12, No. 8, pp. 2164–2169.

(ii) Muhammad Faheem Mushtaq, Sapiee Jamel, Kamaruddin Malik Mohamad, Shamsul Kamal Ahmad Khalid, and Mustafa Mat Deris (2017), "Key Generation Technique based on Triangular Coordinate Extraction for Hybrid Cubes" Journal of Telecommunication, Electronic and Computer Engineering (JTEC). Vol. 9, No. 3–4, pp. 195–200.

(iii) Muhammad Faheem Mushtaq, Sapiee Jamel, Abdulkadir Hassan Disina, Zahraddeen A. Pindar, Mustafa Mat Deris (2017), "A Comprehensive Survey on the Cryptographic Encryption Algorithms" International Journal of Advanced Computer Science and Applications (IJACSA). Vol. 8, No. 11, pp. 333–344.

CHAPTER 1

INTRODUCTION

1.1 Background

Security plays an important role to store information and send it across the network from one location to other with secure manner (Ebrahim, Khan & Khalid, 2013). Hence, the secure communication is the basic requirement of every transaction over networks. Cryptography is an important component to ensure secure communication of data by using the security services like confidentiality, data integrity, access control, authentication and non-repudiation. Data confidentiality refers to the protection of sensitive data from being accessed by unauthorized parties (Savu, 2011).

Cryptography provides a way to protect sensitive information by transferring it into unintelligible and only the authorized receiver can be able to access this information by converting it into the original text. The process to convert the plaintext into ciphertext with the key is called encryption process and to reverse the process of encryption is called decryption process (Kumar & Chaudhary, 2016). The design of cryptographic algorithms should be secure and efficient, low cost, easy to implement and platform independent. Traditionally, the cryptographic algorithms comprises of different mathematical and logical components integrated together as part of the algorithms (Daemen & Rijmen, 2002; Maqsood *et al.*, 2017). The development of fully secured cryptographic algorithm is difficult due to the challenges from cryptanalysts who continuously trying to break any available cryptographic systems. So, the selection of right cryptographic algorithm is essential to accomplish the high-security

requirements to ensure the protection of cryptographic components from cryptanalysis (Jamel, Herawan & Deris, 2010). Furthermore, every cryptographic algorithm needed to fulfill the execution time's test and validation considered as approval with Advanced Encryption Standard (AES) (NIST, 2001).

Cryptography can be further categorized into symmetric key (secret key) encryption and asymmetric key (public key) encryption based on the type of security keys utilized for the encryption or decryption process (Stamp, 2011; Fujisaki & Okamoto, 2013). Furthermore, the symmetric encryption algorithms can be classified into a block and stream cipher by the grouping of message bits (Alshahrani & Walker, 2014). Symmetric key block cipher comprises the five main components: plaintext, encryption and decryption algorithm, ciphertext and key schedule algorithm as shown in Figure 1.1. Moreover, the symmetric block cipher can be further divided into binary and non-binary block cipher based on the final results of the message, keys and ciphertext (Dworkin, 2005). The bit size for the binary block cipher message are 64, 128, 192, and 256, whereas the non-binary block cipher cannot define a standard and depends on the cipher implementation (Baign, Stern & Vaudenay, 2007).

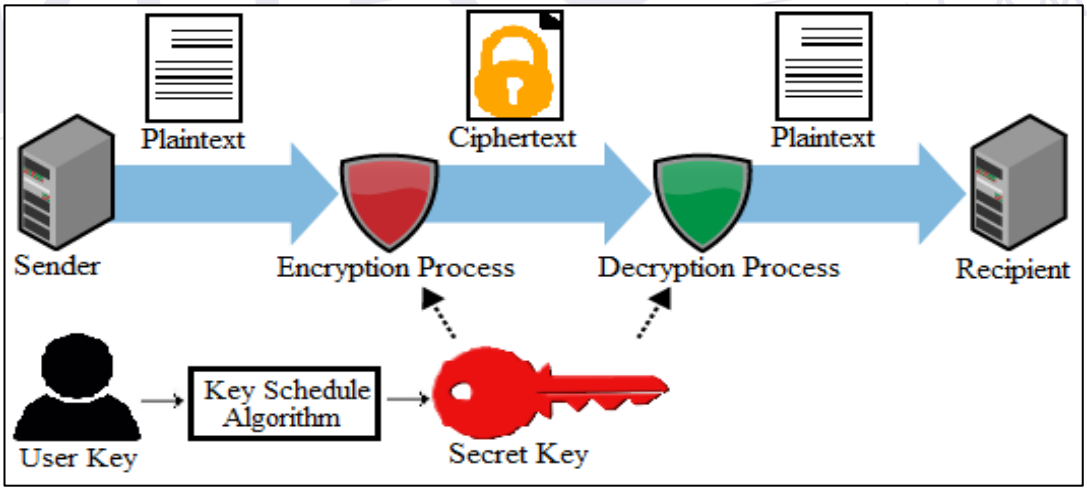

Figure 1.1: Components of Symmetric Block Cipher

Key schedule algorithm is employed to generate secret keys and plays an important role in the development of encryption schemes. In order to resist the related key attack, many researches were conducted to develop a powerful and significant key generation algorithm and increase the difficulty for a cryptanalyst to recover the secret key (Disina *et al*., 2017). All cryptographic algorithms are recommended to follow

128, 192 and 256-bits key lengths proposed by Advanced Encryption Standard (AES) (NIST, 2001). There are three main types of methods that are utilized in the construction of secure encryption and decryption algorithms that contain permutation, substitution, and their combined form.

An image permutation algorithm is based on the geometrical projection and shuffling in the design of key schedule algorithm is used to increases the security of original image by preventing it from outside attacks (Nini & Bouteldja, 2011). Furthermore, the selection of scientific mathematical properties such as orthogonal Latin squares in balanced block mixer and Magic Cube transformation as in image encryption algorithm has proved its significance in strengthening the security of the algorithms (Shen, Jin & Zhou, 2005). The construction of Magic Cubes using the concept of a magic square and two orthogonal Latin squares (Trenkler, 2005). The Magic Cube is 3-Dimensional (3D) coordinates consisting of six faces that are used in the development of complex permutation as apart for the cipher's design.

Hybrid cubes are generated on the basis of Latin squares, Orthogonal Latin Squares, Magic Squares and Magic Cubes (Jamel *et al.*, 2010). This research has been used for further development of new transformation based on permutation of integer numbers and develops a non-binary block cipher. Furthermore, a non-binary block cipher is generated using all possible combination of 2-Dimensional (2D) hybrid cubes as the source for the encryption and decryption keys (Jamel *et al.*, 2011). This research opens up a new way for creating a key schedule algorithm using 3D hybrid cubes based on permutation and combination of integer numbers.

1.2 Problem Statement

Permutation play an important role in the development of ciphers and it contains the finite set of numbers or symbols that are used to mix up readable message into ciphertext as shown in transposition cipher (Kester, 2013). The logic behind any cryptographic algorithm is the number of possible combinations in the key space. The permutations using image encryption algorithm is a very simple combination of row-shift and column-shift operations that makes it easy to be analyzed by cryptanalyst (Li *et al.*, 2008). Moreover, the permutations in positioning for considering flips and twists of the cubes elements which ensures every state of the cube is actually a permuted

(Hoda, 2010). Furthermore, the development of complex permutation which is based on a cube used as a part for the design of cipher. The cubes rotation technique is applied on the image pixels to produce encrypted picture (Diaconu & Loukhaoukha, 2013) and revert the rotation to decrypt the image. These complex permutations provide more security and efficiency in the ciphertext. A Magic Cube based technique is used to achieve information hiding in the grayscale image (Wu *et al.*, 2016). This technique translates the sensitive information into the spatial coordinates and changed the LSBs of the cover image regarding these coordinates. Moreover, the image scrambling technique using the rotation of rows and columns of Magic Cube is used to break the relationship between the image elements, thus create the encryption (Abugharsa, Basari & Almangush, 2014). The limitation of this algorithm is that it uses the same number of rows and columns rotation pattern for the arrangement of blocks as well as the Magic Cube of order 3 are employed that can easily be analyzed by the cryptanalyst (Disina *et al.*, 2017). Hybrid cubes are generated by the combination of two Magic Cubes using inner matrix multiplication of layers which displayed good diffusive characteristics (Jamel *et al.*, 2010). This research opens up a new way of creating a key scheduling algorithm based on the integer numbers.

Many cryptographic algorithms are developed to generate a powerful non-linear encryption key for the block ciphers to withstand the related key attack that makes it difficult for a cryptanalyst to recover the secret key. For that purpose, groups and matrices were employed to proportionately enlarge the key space, thus makes cryptanalysis difficult (Disina *et al.*, 2017). The 2D Hybrid Cube Encryption Algorithm (HiSea) is a non-binary block cipher because the message, ciphertext, encryption and decryption keys, and internal operations of the cipher are based on integer numbers (Jamel *et al.*, 2011). The Rajavel's encryption algorithm and the cubical key are generated using the hybridization and rotation of hybrid cubes by shuffling the cubes (Rajavel & Shantharajah, 2012a). Similarly, the HiSea encryption algorithm performed hybridization with 2D hybrid cubes which are very time-consuming process and it generates the key space that is not sufficient to resist attacks and could easily be exploited. Furthermore, the text scrambling algorithm for encryption based on cube rotation technique has been applied to encrypt text that uses the cube of order 3 which can easily be recovers by the cryptanalyst with minimum number of trails (Rajavel & Shantharajah, 2016). To overcome the limitations, this

research work proposed a new Key Schedule Algorithm based on the coordinate geometry of a Hybrid Cube (KSAHC) for the HiSea encryption algorithm.

1.3 Objectives of the Study

The objectives of this research are as follows:

i. To model a new key schedule algorithm based on the three-dimensional (3D) combination and rotation of hybrid cubes using coordinate geometry.
ii. To integrate the proposed model into non-binary block cipher based on different components such as encryption algorithm, decryption algorithm and key schedule algorithm.
iii. To evaluate the strength of the proposed algorithm using various tests such as Entropy, Brute Force Attack, Correlation assessment, Avalanche effect and NIST test suite.

1.4 Significant of the Study

This research explores the concept of KSAHC algorithm using 3D hybrid cubes for non-binary block cipher which contributes in the following ways:

i. This research needs to come out with geometric coordinates transformation based on circle, square and triangle. The Triangular Coordinate Extraction (TCE) technique is used to extract the value of coordinates during the rotation of *HCs*.
ii. A new Key Schedule Algorithm based on the coordinate geometry of a Hybrid Cube (KSAHC) is proposed. Firstly, the new key matrices of six faces of 3D hybrid cubes are generated using the TCE technique. The ShiftColumns and ShiftRows transformation are performed between the different faces of the hybrid cube. The generation of triangular key matrices based on the rotation point creates the confusion element in the proposed algorithm. The triangular key matrices are invertible and used to generate encryption and decryption keys for the non-binary block cipher.
iii. The implementation of non-binary block cipher based on different component mainly KSAHC algorithm, HiSea encryption and decryption algorithms. The

HiSea encryption algorithm is adopted as the platform to validate the proposed key schedule algorithm.

1.5 Scope of Study

This research concentrates on the development of a new Key Schedule Algorithm based on the rotation of three-dimensional hybrid cube surface using coordinate geometry which can be used in the development of the non-binary block cipher.

1.6 Thesis Organization

This thesis discussed the various aspects involving the design of the new non-binary block cipher. The remaining thesis is comprised as follows:

Chapter 2 describes the literature reviews which is relevant in the design, development and suitable security analysis for Key Schedule Algorithm based on the coordinate geometry of Hybrid Cubes. The earlier part of this chapter will discuss the coordinate geometry, relation on the set, matrices and diagonals. Related works and previous researches have been discussed related to the symmetric block cipher. Various techniques for security analysis of the key schedule algorithm and block cipher are also discussed in this chapter.

Chapter 3 presents the theoretical concepts related to the design of the new KSAHC algorithm for non-binary block cipher and overall design framework of this research. This chapter is divided into two sections. The first section discusses the design and concepts of Triangular Coordinate Extraction technique and the second section outlines the detailed design and integration of KSAHC algorithm into non-binary block cipher.

Chapter 4 contains the security analysis of the proposed KSAHC algorithm to examine its reliability and strength. Several standardized test and attack scenarios used for the test. The results from the analysis are presented and discussed to verify the strength of the proposed algorithm.

Chapter 5 provides the conclusion and future work for further research on symmetric key cryptography.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter describes the cryptographic encryption schemes, mathematical concepts and principles related to coordinate geometry. It includes number, equation and its application can be utilized for the cube rotations. The cube rotation plays an important role in the development of encryption and decryption key. Moreover, the existing encryption and decryption algorithms and its evaluation criteria relevant to the development of the new non-binary cipher are also discussed.

2.2 Preliminaries

This section describes the structure of cryptographic encryption schemes, related mathematical terms, definitions and examples which are relevant in the development of the proposed key schedule algorithm for hybrid cubes.

2.2.1 Overview of a Cryptographic Encryption Schemes

The overview of a cryptographic schemes consists of three algorithms that include key schedule algorithm, encryption algorithm and decryption algorithm. Cryptographic systems can be divided into deterministic and probabilistic encryption scheme

(Goldwasser & Bellare, 2008). Deterministic encryption scheme allows the plaintext is encrypted by using keys that always provide the same ciphertext, but the encryption process is repeated many times. In this scheme, every plaintext has one to one relationship with the keys and ciphertext otherwise it will produce more than one output of particular plaintext during the decryption process. Probabilistic Encryption Scheme shows the plaintext has different ciphertext with the different keys. The probabilistic encryption scheme is significantly secure than the deterministic encryption scheme because it makes difficult for a cryptanalyst to access any sensitive information regarding plaintext that is taken from ciphertext and corresponding key. Furthermore, the cryptographic algorithms can be further divided into two main categories like keyless and key-based cryptosystem as shown in Figure 2.1.

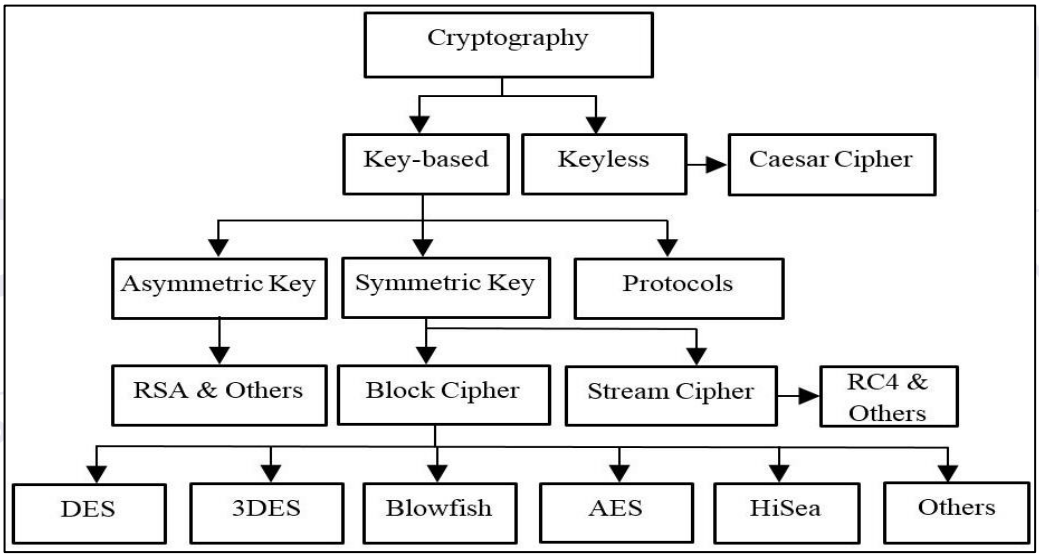

Figure 2.1: Overview of the cryptographic encryption schemes

In the keyless cryptosystem, the relationship between the plaintext and ciphertext having a different version of the message is exclusively depend on the encryption algorithm (Kaushik, Barnela & Kumar, 2012). The keyless cryptosystem is generally less secure than key-based systems because anyone can gain access to the algorithm will be able to decrypt every message that was encoded using keyless cryptosystem such as Caesar cipher (Stallings, 2005). The key-based cryptosystem can be further categories into symmetric key (secret key) encryption and asymmetric key (public key) encryption based on the type of security keys utilized for the encryption or decryption process (Stamp, 2011; Fujisaki & Okamoto, 2013).

The symmetric key (secret key) encryption is employed similar key for the encryption and decryption of a message. Encryption and decryption keys are keeping secret and only known by authorized sender and recipient who want to communicate. The allocation of different keys to the different parties increases the overall message security. The strength of the symmetric key encryption is depending on the secrecy of encryption and decryption keys. The symmetric encryption algorithms can be classified into block and stream cipher on the basis of the grouping of message bits (Alshahrani & Walker, 2014; Dworkin, 2005). In a block cipher, a group of messages characters of a fixed size (a block) is encrypted all at once and sent to the receiver. Moreover, the block cipher can be further divided into binary and non-binary block cipher based on the final results of the message, keys and ciphertext. The message bit size for the binary block cipher are 64, 128, 192, and 256 and the non-binary block cipher has not defined the standard that depends on the cipher implementation.

The block size for the stream cipher is one character and it is not more appropriate for software processing due to the key length as long the message (Sasi, Sivanandam & Emeritus, 2015). The working of the stream cipher is presented in the following steps:

i. A single character of plaintext is combined with a single character from key stream to produce the single character of ciphertext.
ii. The ciphertext character from step 1 sent to the receiver.
iii. Step 1 and step 2 is repeated until the entire message has been sent.

The asymmetric key encryption is commonly referred to as public key encryption in which different keys are employed for the encryption and decryption of the message (Li, 2014). The encryption key is also said as the public key and can be utilized to encrypt the message with the key. The decryption key is said to as secret or private key and can be used to decrypt the message. The strength of the asymmetric key encryption is utilized with a digital signature then it can provide to the users through message authentication detection.

The selection of a symmetric encryption algorithm instead of the asymmetric encryption algorithm because its implementation is very fast, efficient, effective and simple to employ for encryption and decryption process. Furthermore, the AES is a symmetric block cipher employed for encryption and decryption of message adopted

REFERENCES

Abugharsa, A. B., Basari, A. S. B. H., & Almangush, H. M. (2014). A New Image Scrambling Technique using Block Rotation Algorithm based on Rubik's Cube. *Australian Journal of Basic and Applied Sciences*, 7(14), pp. 97–108.

Acharya, B., Sharma, M. D., Tiwari, S., & Minz, V. K. (2010). Privacy protection of biometric traits using modified Hill Cipher with involutory key and robust cryptosystem. *Procedia Computer Science*, 2, pp. 242–247.

Aguilera, A., & Aguila, R. P. (2004). General n-dimensional rotations. In *WSCG Short Communication Papers Proceedings*, pp. 1–8.

Ahmad, J., Ahmed, F., 2012. Efficiency analysis and security evaluation of image encryption schemes. *International Journal of Video & Image Processing and Network Security*, 12(4), pp. 18–31.

Ahmad, H., Hassan, A., Saeb, M., & Hamed, H. D. (2005). The PYRAMIDS Block Cipher. *International Journal of Network Security*, 2, pp. 50–60.

Aiden A. Bruen and Mario A. Forcinito. (2005). *Cryptography, Information Theory, and Error-Correction*. John Wiley & Sons, Inc.

Akhavan, A., Samsudin, A., & Akhshani, A. (2013). A novel parallel hash function based on 3D chaotic map. *Eurasip Journal on Advances in Signal Processing*, pp. 1–12.

Alshahrani, A. M., & Walker, S. (2014). Implement A Novel Symmetric Block Cipher Algorithm. *International Journal on Cryptography and Information Security*, 4(4), pp. 1–11.

Andreeva, E. I. (2005). *Analysis and Design of Authenticated Encryption Modes*. Master Thesis, University of Saarland, Germany.

Anghel, N. (2014). Determinant Identities and the Geometry of Lines and Circles. *Analele Stiintifice Ovidius Constanta, Versita*, 22(2), pp. 37–49.

Anton, H., & Rorres, C. (2014). *Elementary Linear Algebra.* 11th ed. John Wiley and Sons, Inc.

Applebaum, B., Avron, J., & Brzuska, C. (2017). Arithmetic Cryptography. *Journal of the ACM*, 64(2), pp. 1–74.

Azad, S., & Pathan, A. S. K. (2014). *Practical Cryptography: Algorithms and Implementations Using C++*. CRC Press, USA.

Baign, T., Stern, J., & Vaudenay, S. (2007). Linear Cryptanalysis of Non Binary Ciphers with an Application to SAFER. In *Proceedings of the 14th International Conference on Selected Areas in Cryptography*, pp. 184–211.

Biryukov, A., Dunkelman, O., Keller, N., Khovratovich, D., & Shamir, A. (2010). Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds. In *EUROCRYPT'10 Proceedings of the 29th Annual international conference on Theory and Applications of Cryptographic Techniques*, pp. 299–319.

Campbell, J. (2016). *Cryptography, Network Exploitation, Crime & Policy Impact*. Saint Leo University.

Clark, E. (2001). *Elementary Abstract Algebra*. Mathematics department, University of South Florida, pp. 1–97.

Daemen, J., & Rijmen, V. (2002). *The Design of Rijndael - The Advanced Encryption Standard*. Springer-Verlag Berlin Heidelberg, New York.

Daemen, J., & Rijmen, V. (2013). *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media.

Diaconu, A. V., & Loukhaoukha, K. (2013). An improved secure image encryption algorithm based on rubik's cube principle and digital chaotic cipher. *Mathematical Problems in Engineering*, 1, pp. 1–10.

Disina, A. H., Jamel, S., Aamir, M., Pindar, Z. A., Deris, M. M., & Mohamad, K. M. (2017). A Key Scheduling Algorithm Based on Dynamic Quasigroup String Transformation and All-Or- Nothing Key Derivation Function. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, 9(3–5), pp. 1–6.

Disina, A. H., Jamel, S., Pindar, Z. A., & Deris, M. M. (2016). All-or-nothing Key Derivation Function Based on Quasigroup String. In *Proceeding of IEEE International Conference on Information Science and Security (ICISS)*, pp. 6–10.

Dworkin, M. (2005). Recommendation for Block Cipher Modes of Operation. *NIST Special Publication 800-38B*, pp. 1-16.

Ebrahim, M., Khan, S., & Khalid, U. Bin. (2013). Symmetric Algorithm Survey: A Comparative Analysis. *International Journal of Computer Applications*, 61(20), pp. 12–19.

Edelman, A., & Strang, G. (2015). Random Triangle Theory with Geometry and Applications. *Foundations of Computational Mathematics,* 15(3), pp. 681-713.

Feng, X., Tian, X., & Xia, S. (2011). An Improved Image Scrambling Algorithm Based On Magic Cube Rotation and Chaotic Sequences. In *Proceeding of IEEE 4th International Congress on Image and Signal Processing*, pp. 1021–1024.

Fujisaki, E., & Okamoto, T. (2013). Secure integration of asymmetric and symmetric encryption schemes. *Journal of Cryptology*, 26(1), pp. 80–101.

Gaurav, K., Pal, K., & Dilbahar, S. (2013). Change in the Key Expansion Function of AES. *International Journal of Innovative Technology and Exploring Engineering*, 2(4), pp. 267–269.

Goldwasser, S., & Bellare, M. (2008). *Lecture Notes on Cryptography*. MIT Computer Science and Artificial Intelligence Laboratory, Cambridge, Massachusetts, USA.

Granboulan, L., Levieil, E., & Piret, G. (2006). Pseudorandom Permutation Families over Abelian Groups. *Fast Software Encryption*, 4047, pp. 57–77.

Haber, H. (2012). *Three-Dimensional Rotation Matrices*. In Physics 216, pp. 1–18. Retrieved on December 2, 2017, from http://scipp.ucsc.edu/~haber/ph116A /rotation_11.pdf

Hamza, A. M., & Imran, B. K. (2017). Orthogonal of Type I Matrices with Application. *Applied Mathematical Sciences*, 11(40), pp. 1983–1994.

Hearn, D., & Baker, M. P. (2005). *Computer Graphics - C version*. Pearson Education.

Hill, J., Thron, C. (2017). *Elementary Abstract Algebra : Examples and Applications*. Creative Commons Attribution 4.0 International license, USA.

Hoda, R. (2010). Finding the total number of legal permutations of the Rubik's Cube, In *Extended Essay – Mathematics*. pp. 1-32.

Horn, R. A., & Johnson, C. R. (2013). *Matrix Analysis*. 2nd Ed. Cambridge University Press New York, USA.

ISO/IEC-18033-3. (2005). Information technology- Security techniques- Encryption algorithms-Part 3: Block ciphers. *International Standard ISO / IEC*.

ISO (International Organization for Standardization). (2013). *International Standard ISO / IEC Information technology - Security techniques - Privacy framework*.

Jamel, S. (2012). *The Hybrid Cubes Encryption Algorithm (HiSea)*. Ph.D Thesis, Universiti Tun Hussein Onn Malaysia (UTHM), Johor, Malaysia, pp. 1–138.

Jamel, S., Deris, M. M., Tri, I., Yanto, R., & Herawan, T. (2011). HiSea : A Non Binary Toy Cipher. *Journal of Computing*, 3(6), pp. 20–27.

Jamel, S., Deris, M. M., Yanto, I. T. R., & Herawan, T. (2011). The hybrid cubes encryption algorithm (HiSea). *Communications in Computer and Information Science, Springer-Verlag Berlin Heidelberg*, 154, pp. 191–200.

Jamel, S., Herawan, T., & Deris, M. M. (2010). A cryptographic algorithm based on hybrid cubes. *Computational Science and Its Applications ICCSA*, 6019, pp. 175–187.

Jia, Y.-B. (2017). *Rotation in the Space*. In Problem Solving Techniques for Applied Computer Science, pp. 1–13.

Jindal, P., & Singh, B. (2015). Analyzing the security-performance tradeoff in block ciphers. *International Conference on Computing, Communication and Automation, ICCCA*, pp. 326–331.

Kaushik, A., Barnela, M., & Kumar, A. (2012). Keyless User Defined Optimal Security Encryption. *International Journal of Computer and Electrical Engineering*, 4(2), pp. 2–6.

Kester, Q.-A. (2013). A Hybrid Cryptosystem Based on Vigenere Cipher and Columnar Transposition Cipher. *International Journal of Advanced Technology & Engineering Research (IJATER)*, 3(1), pp. 141–147.

Kim, S.-J., Umeno, K., & Hasegawa, A. (2004). Corrections of the NIST Statistical Test Suite for Randomness. *Journal of Cryptology*, 18(6), pp. 1367–1379.

Koscielny, C. (2002). Generating quasigroups for cryptographic applications. *International Journal of Applied Mathematics and Computer Science*, 12(4), pp. 559–570.

Kuhnel, W. (2015). *Differential Geometry.* 3rd Ed. American Mathematical Society.

Kumar, A., & Tewari, R. R. (2017). Expansion of Round Key Generations in Advanced Encryption Standard for Secure Communication. *International Journal of Computational Intelligence Research*, 13(7), pp. 1679–1698.

Kumar, N., & Chaudhary, P. (2016). Performance evaluation of encryption/decryption mechanisms to enhance data security. *Indian Journal of Science and Technology*, 9(20), pp. 1-10.

Kumar, P. R., Sailaja, K. L., Dhenakaran, S. S., & Saikishore, P. (2012). Chakra: A new approach for symmetric key encryption. In *Proceedings of the 2012 World Congress on Information and Communication Technologies (WICT)*, pp. 727–732.

Kreyszig, E., Kreyszig, H., & Norminton, E. J. (2010). *Advanced Engineering Mathematics.* 10th Ed. John Wiley and Sons, Inc.

Li, C., Li, S., Chen, G., & Halang, W. A. (2008). Cryptanalysis of an image encryption scheme based on a compound chaotic sequence. *Image and Vision Computing*, 27(8), pp. 1035–1039.

Li, N. (2014). Asymmetric Encryption. *Encyclopedia of Database Systems. Springer, New York.*

Luo, L., Xu, D., Zhang, Z., Zhang, J., & Qu, W. (2013). A fast and robust circle detection method using perpendicular bisector of chords. *25th Chinese Control and Decision Conference (CCDC)*, 3, pp. 2856–2860.

Maldacena, J., Seiberg, N., & Moore, G. (2001). Geometrical interpretation of D-branes in gauged WZW models. *Journal of High Energy Physics*, 7, pp. 1–62.

Maqsood, F., Ali, M. M., Ahmed, M., & Shah, M. A. (2017). Cryptography : A Comparative Analysis for Modern Techniques. *International Journal of Advanced Computer Science and Applications*, 8(6), pp. 442–448.

Mel, H. X., & Baker., D. M. (2001). *Cryptography decrypted*. Addison-Wesley Professional.

Mushtaq, M. F., Jamel, S., & Deris, M. M. (2017). Triangular Coordinate Extraction (TCE) for Hybrid Cubes. *Journal of Engineering and Applied Sciences*, 12(8), pp. 2164–2169.

Mushtaq, M. F., Jamel, S., Disina, A. H., Pindar, Z. A., Shakir, N. S. A., & Deris, M. M. (2017). A Comprehensive Survey on the Cryptographic Encryption Algorithms. *International Journal of Advanced Computer Science and Applications*, 8(11), pp. 333–344.

Mushtaq, M. F., Jamel, S., Mohamad, K. M., Khalid, S. K. A., & Deris, M. M. (2017). Key Generation Technique based on Triangular Coordinate Extraction for Hybrid Cubes. *Journal of Telecommunication, Electronic and Computer Engineering*, 9(3–4), pp. 195–200.

Nini, B., & Bouteldja, D. (2011). Virtual Cylindrical View of a Color Image for its

Permutation for an Encryption Purpose. *International Journal of Computer Applications*, 16(1), pp. 11–17.

NIST. (2015). Frequency test. Retrieved on 13 October, 2015, from https://www.itl.nist.gov/div898/software/dataplot/refman1/auxillar/freqtest.htm

NIST, N. I. of S. (2001). *Advanced Encryption Standard (AES)*. Federal Information Processing Standards Publication 197, pp. 1-47.

Pop, V., & Furdui, O. (2017). *Square matrices of order 2: Theory, Applications, and Problems*. 1st Ed. Springer International Publishing.

Rajavel, D., & Shantharajah, S. (2016). Scrambling algorithm for encryption of text using cube rotation artificial intelligence technique. *Biomedical Research*, pp. 251–256.

Rajavel, D., & Shantharajah, S. P. (2012a). Cryptography Based on Combination of Hybridization and Cube's Rotation. *International Journal of Computational Intelligence and Informatics*, 1(4), pp. 294–299.

Rajavel, D., & Shantharajah, S. P. (2012b). Cubical Key Generation and Encryption Algorithm Based on Hybrid Cube's Rotation. In *Proceedings of the International Conference on Pattern Recognition, Informatics and Medical Engineering*, pp. 183–187.

Ramanujam, S., & Karuppiah, M. (2011). Designing an algorithm with high Avalanche Effect. *International Journal of Computer Science and Network Security*, 11(1), pp. 106–111.

Rihan, S. D., Osman, S. E. F., & Khalid, A. (2015). A Performance Comparison of Encryption Algorithms AES and DES. *Intetnational Journal of Engineering Research & Technology*, 4(12), pp. 151–154.

Robbin, J. W. (2005). *Coordinate Geometry*. University of Wisconsin-Madison. http://doi.org/10.2307/3603154.

Rosen, K. (2011). *Discrete Mathematics and Its Applications*. McGraw-Hill. http://doi.org/1439880182.

Rukhin, A., Soto, J., Nechvatal, J. R., Smid, M. E., Barker, E. B., Leigh, S. D., Levenson, M., Vangel, M., Banks, D. L., Heckert, N. A., Dray, J. F., Vo, S. (2010). A statistical test suite for random and pseudorandom number generators for cryptographic applications. *National Institute of Standards and Technology*, pp. 1–82.

Sasi, S. B., Sivanandam, N., & Emeritus. (2015). A survey on cryptography using optimization algorithms in WSNs. *Indian Journal of Science and Technology*, 8(3), pp. 216–221.

Sastry, V. U. K., Shankar, N. R., & Bhavani, S. D. (2013). A Large Block Cipher Involving Key Dependent Permutation, Interlacing and Iteration. *Cybernetics And Information Technologies*, 13(3), pp. 50–63.

Savu, L. (2011). Cryptography Role in Information Security. *Recent Researches in Communications and Information Technology*, pp. 36–41.

Schneier, B. (2010). *Crypto Engineering Design Principles and Practical Applications*. Wiley Publishing Inc.

Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C., & Ferguson, N. (1999). *The Twofish encryption algorithm: a 128-bit block cipher*. John Wiley & Sons, Inc.

Serre, D. (2010). *Matrices: Theory and Application*. Springer Berlin Heidelberg London.

Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28(4), pp. 656–715.

Shen, J., Jin, X., & Zhou, C. (2005). A color image encryption algorithm based on magic cube transformation and modular arithmetic operation. *Advances in Multimedia Information Processing*, *3768*, pp. 270–280.

Singh, A., Agarwal, P., & Chand, M. (2017). Analysis of Development of Dynamic S-Box Generation. *Computer Science and Information Technology*, 5(5), pp. 154–163.

Single, E., & Mccallum, M. H. G. (2015). *Calculus Single and Multivariable*. 6th Ed. Wiley Publishing Inc.

Stallings, W. (2005). *Cryptography and Network Security: Principles and Practices*. *Cryptography and Network Security*. Prentice Hall.

Stallings, W. (2006). *Cryptography and Network Security*. Prentice Hall.

Stamp, M. (2011). *Information Security: Principles and Practice*. John Wiley & Sons.

T. Baigneres, P. Junod, Y. Lu, J. Monnerat, S. V. (2006). *A Classical Introduction To Cryptography Exercise*. Springer Berlin Heidelberg.

Trenkler, M. (2000). A construction of magic cubes. *The Mathematical Gazette*, 84, pp. 36–41.

Trenkler, M. (2005). An algorithm for making magic cubes. *The Pi ME Journal*, 12(2), pp. 105–106.

Vince, J. (2005). *Geometry for computer graphics*. *Geometry for Computer Graphics: Formulae, Examples and Proofs*. http://doi.org/10.1007/b138852

Weisstein, E. (2017). Diagonal. Retrieved on 29 November, 2017, from http://mathworld.wolfram.com /Diagonal.html.

Wu, Q., Zhu, C., Li, J. J., Chang, C. C., & Wang, Z. H. (2016). A magic cube based information hiding scheme. *Journal of Information Security and Application*, 26, pp. 1–7.

Xu, Z. D. Q. (2015). The Design of A Key Expansion Algorithm Based On Dynamic Dislocation Counts. In *Proceeding of the IEEE 11th International Conference on Computational Intelligence and Security.* pp. 345-349.

Ye, H., Shang, G., Wang, L., & Zheng, M. (2016). A new method based on hough transform for quick line and circle detection. In *Proceeding of the 8th International Conference on BioMedical Engineering and Informatics*, pp. 52–56.

Yu, Z., Meng, T., Dai, Z., & Yang, X. (2006). Design and Implementation of Reconfigurable Shift Unit using FPGAs. *International Symposium on Pervasive Computing and Applications*, pp. 543–545.